AMENDMENTS TO THE CLAIMS

1.   (Original) In a networked server having a file system therein, a virus detection monitoring system comprising:

a) a check-in interceptor configured to monitor the network server for incoming files and intercept incoming files before said files are transferred to the file system of the server; and

b) an anti-virus interface operatively coupled to said check-in interceptor, said anti-virus interface configured to transfer the incoming files which are intercepted to an anti-virus application for virus detection and removal.

2.   (Original) The virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a signal indicating whether a virus was detected in the intercepted incoming file and whether the virus was removed.

3.   (Original) The virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file.

4.   (Original) The virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application.

5.   (Original) The virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a

2

signal indicating whether a virus was detected in the intercepted incoming file, said check-in interceptor further configured to communicate the signal to a user submitting the intercepted incoming file.

6.   (Original) The virus detection monitoring system of claim 1, further comprising a "dat file updater and validater" coupled to the anti-virus application, said dat file updater and validater configured to periodically download updated virus data, validate the updated virus data after download, and update said anti-virus application with said updated virus data after validating said virus data.

7.   (Previously Presented) The virus detection monitoring system of claim 1, wherein said check-in interceptor inspects documents and files uploaded to an electronic document control system operating on the network server.

8.   (Original) The virus detection monitoring system of claim 1, wherein said check-in interceptor intercepts document upload commands issued to the network server.

9.   (Previously Presented) The virus detection monitoring system of claim 8, wherein said document upload commands comprise hypertext transfer protocol commands.

10.   (Previously Presented) In a networked server having a file system therein, a method for virus detection monitoring comprising:

    a) intercepting incoming files before the incoming files are transferred to the file system of the server; and

b) transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal.

11. (Previously Presented) The method of claim 10, further comprising preventing an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file.

12. (Previously Presented) The method of claim 10, further comprising preventing an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application.

13. (Original) The method of claim 10, further comprising:

a) receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file; and

b) communicating the signal to a user submitting the intercepted incoming file.

14. (Previously Presented) The method of claim 10, further comprising:

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

15. (Original) The method of claim 10, wherein said network server comprises an electronic document control system.

16. (Previously presented) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for virus detection monitoring, said method comprising:

a) intercepting incoming files before the files are transferred to a file system of a server; and

b) transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal.

17. (Previously Presented) The program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file.

18. (Previously Presented) The program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application.

19. (Original) The program storage device of claim 16, said method further comprising:

a) receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file; and

b) communicating the signal to a user submitting the intercepted incoming file.

20. (Previously Presented) The program storage device of claim 16, said method further comprising:

5

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

21.   (Original) The program storage device of claim 16, wherein said network server comprises an electronic document control system.

22.   (Previously Presented) In a networked server having a file system therein, a virus detection monitoring system comprising:

a) means for intercepting incoming files before the incoming files are transferred to the file system of the server; and

b) means for transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal.

23.   (Original) The virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file.

24.   (Original) The virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application.

25.   (Original) The virus detection monitoring system of claim 22, further comprising:

a) means for receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file; and

b) means for communicating the signal to a user submitting the intercepted incoming file.

26.   (Original) The virus detection monitoring system of claim 22, further comprising:

a) means for downloading updated virus data according to a schedule;

b) means for validating the updated virus data; and

c) means for updating said anti-virus application with said updated virus data.

27.   (Original) The virus detection monitoring system of claim 22, wherein said network server comprises an electronic document control system.